UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

VANESSA HAYS, individually and on behalf of all others similarly situated, Plaintiff, v. INTERNATIONAL BUSINESS MACHINES CORPORATION and JOHNSON & JOHNSON HEALTH CARE SYSTEMS, INC., Defendant.	Case No. _____ **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Vanessa Hays ("Plaintiff") brings this Class Action Complaint ("Complaint") against International Business Machines Corporation ("IBM") and Johnson & Johnson Health Care Systems, Inc. ("Janssen," and collectively with IBM, "Defendants"), as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions and her counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This class action arises out of the recent ransomware attack and data breach ("Data Breach") resulting from Defendants' failure to implement reasonable and industry standard data security practices.

2. Defendant Janssen is a subsidiary of Johnson & Johnson and through its Janssen CarePath program "provides access, affordability, and treatment support resources to help patients get started on, and stay on, the Janssen medications their healthcare providers prescribe."[1] In 2022

[1] https://www.janssen.com/us/patient-resources/support-programs (last accessed Oct. 6, 2023).

alone, "Janssen helped more than 1.16 million patients in the U.S. through the Janssen CarePath program."[2]

3. Defendant IBM "provides hybrid cloud and artificial intelligence (AI), and business services; its integrated solutions and products use data and information technology in industries and business processes."[3]

4. Plaintiff's and Class Members' sensitive personal information—which they entrusted to Defendant with the mutual understanding that Defendant would protect it against disclosure—was compromised and unlawfully accessed due to the Data Breach.

5. Defendants collected and maintained certain personally identifiable information and/or protected health information of Plaintiff and putative Class Members (defined below), who are (or were) patients enrolled in the Janssen CarePath program.

6. On or about August 2, 2023, Defendants became aware that there was unauthorized access to personal information in a database managed by Defendants.

7. The private information compromised in the Data Breach included Plaintiff's and Class Members' personally identifiable information ("PII") and medical and health insurance information, which is protected health information ("PHI", and collectively with PII, "Private Information") as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). On information and belief, the Private Information included contact information, health insurance information, and information about medications and associated conditions that were provided to the Jansen CarePath application during Defendant Janssen's provision of services to Plaintiff and Class Members.

[2] *Id.*
[3] https://www.forbes.com/companies/ibm/?sh=bf26c8539c45 (last accessed Oct. 6, 2023).

8. The Private Information compromised in the Data Breach was exfiltrated by cyber-criminals and remains in the hands of those cyber-criminals who target Private Information for its value to identity thieves.

9. Defendants failed to notify Plaintiff and Class Members that their Private Information was compromised for nearly two months.

10. As a result of the Data Breach, Plaintiff and Class Members suffered concrete injuries in fact including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

11. The Data Breach was a direct result of Defendants' failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect patients' Private Information from a foreseeable and preventable cyberattack.

12. Defendants maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendants' computer network and servers in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus, Defendant was on notice that failing to

take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

13. Defendants disregarded the rights of Plaintiff and Class Members by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure their data systems were protected against unauthorized intrusions; failing to disclose that they did not have adequately robust computer systems and security practices to safeguard Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

14. Plaintiff's and Class Members' identities are now at risk because of Defendants' negligent conduct because the Private Information that Defendants collected and maintained is now in the hands of data thieves.

15. Armed with the Private Information accessed in the Data Breach, data thieves can engage in identity theft and fraud and can in the future commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

16. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

17. Plaintiff and Class Members may also incur out of pocket costs, *e.g.*, for purchasing credit monitoring services, credit freezes, credit reports, or other protective measures

to deter and detect identity theft.

18. Plaintiff brings this class action lawsuit on behalf of all those similarly situated to address Defendants' inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to unauthorized access by an unknown third party and precisely what specific type of information was accessed.

19. Plaintiff's claims are brought as a class action, pursuant to Federal Rule of Civil Procedure 23, on behalf of herself and all other similarly situated persons. Plaintiff seeks relief in this action individually and on behalf of a similarly situated class of individuals for negligence, breach of implied contract, unjust enrichment, bailment, and breach of fiduciary duty. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

20. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

21. Plaintiff seeks remedies including, but not limited to, compensatory damages and injunctive relief including improvements to Defendants' data security systems, future annual audits, and adequate credit monitoring services funded by Defendants.

PARTIES

22. Vanessa Hays is a natural person, resident, and citizen of the State of Tennessee.

23. Defendants obtained and continue to maintain the Private Information of Plaintiff and owed her a legal duty and obligation to protect her Private Information from unauthorized access and disclosure. Plaintiff's Private Information was compromised and disclosed as a result

of Defendants' inadequate data security practices, which resulted in the Data Breach.

24. Plaintiff recalls receiving a notice letter dated September 15, 2023, from Defendants, stating that an unauthorized party downloaded Plaintiff's Private Information which she had previously provided to Defendant Janssen.

25. Defendant International Business Machines Corporation is a New York corporation with its principal place of business at One Orchard Road, Armonk, New York 10504.

26. Defendant Johnson & Johnson Health Care Systems Inc. which owns and operates Janssen CarePath is incorporated in the State of New Jersey with its principal place of business at 425 Hoes Lane Piscataway, New Jersey 08854.

JURISDICTION AND VENUE

27. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and Plaintiff and at least one member of the class is a citizen of a state different from Defendants.

28. This Court has personal jurisdiction over Defendants because their principal place of business is in this District and/or they regularly conduct business in the State where this District is located, have sufficient minimum contacts in this State, and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

29. Venue is proper under 18 U.S.C § 1391(b) because a substantial part of the events that gave rise to Plaintiff's claims took place within this district and Defendant IBM's principal place of business is in this District.

FACTUAL ALLEGATIONS

Background

30. Defendant Janssen is a subsidiary of Johnson & Johnson and through its Janssen CarePath program "provides access, affordability, and treatment support resources to help patients get started on, and stay on, the Janssen medications their healthcare providers prescribe."[4] In 2022 alone, "Janssen helped more than 1.16 million patients in the U.S. through the Janssen CarePath program."[5]

31. Defendant IBM is a service provider to Janssen, and according to Defendants "manages the application and the third-party database that supports Janssen CarePath."[6]

32. Plaintiff and Class Members are current and former patients who were enrolled on Defendant Janssen's "Janssen CarePath" patient support platform. Janssen CarePath "offers different savings options and resources at no cost to patients to help them learn about, afford, and stay on their medication. It includes the Janssen CarePath Savings Program, Janssen CarePath account, and other helpful resources that are specific to each Janssen medicine."[7]

33. While obtaining services from Defendant Janssen, patients, including Plaintiff and Class Members, provided Defendant Janssen with at least their PII and PHI, either directly or through their healthcare providers.

34. Upon information and belief, while collecting Private Information from patients, including Plaintiff, Defendant Janssen promised to provide confidentiality and adequate security for patient data through its applicable privacy policy and through other disclosures in compliance

[4] https://www.janssen.com/us/patient-resources/support-programs (last accessed Oct. 6, 2023).
[5] *Id.*
[6] *Data Breach Notice*, Ex. A.
[7] https://www.janssencarepath.com/ (last accessed Oct. 6, 2023).

with statutory privacy requirements.

35. Indeed, the Privacy Policy posted on Defendant Janssen's website provides that Defendant Janssen "respects your privacy" and claims that "[w]e seek to use reasonable organizational, technical, and administrative measures designed to protect personal information under our control."[8]

36. Plaintiff and Class Members, as former and current patients, and members of Defendant Janssen's CarePath program, relied on these promises and on this sophisticated business entity and its business associate, Defendant IBM, to keep their sensitive Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Patients, in general, demand security to safeguard their Private Information, especially when PHI and other sensitive private information is involved.

The Data Breach

37. On or around August 2, 2023, Defendant Janssen "became aware of a technical method by which unauthorized access to the database [containing Plaintiff's and Class Members' Private Information] could be obtained."[9] Defendant Janssen then "immediately notified IBM, and, working with the third-party database provider, IBM promptly remediated the issue."[10] Defendant IBM "also undertook an investigation to assess whether there had been unauthorized access to the database."[11]

[8] https://www.janssencarepath.com/privacy-policy (last accessed Oct. 6, 2023).
[9] *See Data Breach Notice*, Ex. A.
[10] *Id.*
[11] *Id.*

38. As a result of its investigation, Defendant IBM determined "on August 2, 2023, that there was unauthorized access to personal information in the database."[12]

39. According to Defendants:

> The personal information involved in this incident may have included your name and one or more of the following: contact information, health insurance information, and information about medications and associated conditions that were provided to the Jansen CarePath application.[13]

40. Defendants failed to notify Plaintiff and Class Members that their Private Information was compromised in the Data Breach for approximately two months.[14]

41. Upon information and belief, the cyberattack was targeted at Defendant Janssen, due to its status as a healthcare entity that collects, creates, and maintains Private Information on its computer networks and/or systems.

42. Upon information and belief, Plaintiff's and Class Members' Private Information was compromised and acquired in the Data Breach.

43. The files containing Plaintiff's and Class Members' Private Information, that were targeted and stolen from Defendants, included their PII and/or PHI.

44. Because of this targeted cyberattack, data thieves were able to gain access to and obtain data from Defendants that included Plaintiff's and Class Members' Private Information.

45. As evidenced by the Data Breach's occurrence, the Private Information contained in Defendants' network and servers was not encrypted. Had the information been properly encrypted, the data thieves would have exfiltrated only unintelligible data.

---

[12] *Id.*
[13] *Id.*
[14] *See id.* dated Sept. 15, 2023, but not received by Plaintiff until October, 2023.

46. Plaintiff further believes that her PII and that of Class Members was or soon will be published to the dark web, where it will be available for purchase, because that is the *modus operandi* of cybercriminals.

47. Defendants had obligations created by the FTC Act, HIPAA, contract, state and federal law, common law, and industry standards to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

Data Breaches are Preventable

48. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members such as encrypting the information or deleting it when it is no longer needed, causing the exposure of Private Information.

49. Defendants could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing Private Information.

50. To prevent and detect cyberattacks and/or ransomware attacks Defendants could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, patients and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[15]

51. To prevent and detect cyberattacks or ransomware attacks Defendants could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

[15] *Id.* at 3-4.

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[16]

52. Given that Defendants were storing the Private Information of current and former patients, Defendants could and should have implemented all the above measures to prevent and detect cyberattacks.

[16] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Nov. 11, 2021).

53. The occurrence of the Data Breach indicates that Defendants failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and, upon information and belief, the exposure of the Private Information of potentially millions of patients, including that of Plaintiff and Class Members.[17]

Defendants Acquire, Collect, and Store Patients' Private Information

54. Defendants acquire, collect, and store a massive amount of Private Information on patients, former patients, and other personnel enrolled in Defendant Janssen's CarePath program.

55. As a condition of obtaining patient support services from Defendant Janssen, Defendant Janssen requires that patients entrust it with highly sensitive personal information.

56. By obtaining, collecting, and using Plaintiff's and Class Members' Private Information, Defendant Janssen assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.

57. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and would not have entrusted it to Defendants absent a promise to safeguard that information.

58. Plaintiff and Class Members relied on Defendants to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Defendants Knew or Should Have Known of the Risk Because Healthcare Entities in Possession of Private Information are Particularly Suspectable to Cyber Attacks

[17] https://www.databreachtoday.com/group-claims-stole-25-million-patients-data-in-attack-a-23212 (last accessed Oct. 5, 2023).

59. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches targeting healthcare entities and their business associates which collect and store Private Information, like Defendants, preceding the date of the Data Breach.

60. Data breaches, including those perpetrated against healthcare entities that store Private Information in their systems, have become widespread.

61. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[18]

62. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendant Janssen knew or should have known that its electronic records would be targeted by cybercriminals.

63. Defendants knew and understood unprotected or exposed Private Information in the custody of healthcare entities and their business associates, like Defendants, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that Private Information through unauthorized access.

[18] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6.

64. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendants' data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a data breach.

65. Indeed, cyberattacks, such as the one experienced by Defendants, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store Private Information are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[19]

66. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

67. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for Plaintiff's and Class Members' Private Information.

68. The ramifications of Defendants' failure to keep secure Plaintiff's and Class Members' Private Information are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

[19] https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last accessed Oct. 17, 2022).

69. As a healthcare entity and business associate in custody of current and former patients' Private Information, Defendants knew, or should have known, the importance of safeguarding Private Information entrusted to them by Plaintiff and Class Members, and of the foreseeable consequences if their data security systems were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a data breach. Defendants failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

Value of Private Information

70. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[20] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[21]

71. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[22]

[20] 17 C.F.R. § 248.201 (2013).
[21] *Id.*
[22] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Oct. 17, 2022).

72. For example, PII can be sold at a price ranging from $40 to $200.[23] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[24]

73. PII can sell for as much as $363 per record according to the Infosec Institute.[25] PII is particularly valuable because criminals can use it to target victims with frauds and scams.

74. Identity thieves use stolen PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

75. Theft of PHI is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."

76. According to account monitoring company LogDog, medical data sells for $50 and up on the Dark Web.[26]

77. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. Upon information and belief, the information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

---

[23] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Oct. 17, 2022).
[24] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Oct. 217, 2022).
[25] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited May 7, 2023).
[26] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content (last accessed July 20, 2021)

78. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information. .. [is] worth more than 10x on the black market."[27]

79. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

80. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[28]

Defendants Fail to Comply with FTC Guidelines

81. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

82. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines

---

[27] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Oct. 17, 2022).

[28] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited Oct. 5, 2023).

note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[29]

83. The guidelines also recommend that healthcare businesses use an intrusion detection system to expose a data breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[30]

84. The FTC further recommends that healthcare companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

85. The FTC has brought enforcement actions against healthcare entities for failing to protect patient data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential patient data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

---

[29] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Oct. 5, 2023).
[30] *Id.*

86. These FTC enforcement actions include actions against healthcare providers like Defendant. *See, e.g., In the Matter of LabMd, Inc., A Corp*, 2016-2 Trade Cas. (McLaren) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

87. Defendants failed to properly implement basic data security practices.

88. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

89. Upon information and belief, Defendants were at all times fully aware of their obligation to protect the Private Information of patients. Defendants were also aware of the significant repercussions that would result from its failure to do so.

Defendants Fail to Comply with HIPAA Guidelines

90. Defendants are covered entities under HIPAA (45 C.F.R. § 160.102) and are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

91. Indeed, Defendants acknowledge as much in a "Business Associate Agreement" signed by IBM in September 2022.[31]

92. Defendants are subject to the rules and regulations for safeguarding electronic

[31] *See Business Associate Agreement*, https://www.janssencarepath.com/sites/www.janssencarepath-v1.com/files/ibm-platform-business-associate-agreement.pdf (last visited Oct. 6, 2023).

forms of medical information pursuant to the Health Information Technology Act ("HITECH").[32] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

93. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

94. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

95. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

96. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

97. HIPAA's Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

[32] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

d. Ensure compliance by its workforce.

98. HIPAA also requires Defendants to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendants are required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

99. HIPAA and HITECH also obligate Defendants to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

100. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendants to provide notice of the Data Breach to each affected individual "without unreasonable delay and *in no case later than 60 days following discovery of the breach*."[33]

101. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

[33] Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added).

102. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

103. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material.[34] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says, "represent the industry standard for good business practices with respect to standards for securing e-PHI." US Department of Health & Human Services, Guidance on Risk Analysis.[35]

Defendants Fail to Comply with Industry Standards

104. As noted above, experts studying cybersecurity routinely identify healthcare entities in possession of Private Information as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

105. Several best practices have been identified that, at a minimum, should be implemented by healthcare entities in possession of Private Information, like Defendants,

[34] http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html.
[35] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendants failed to follow these industry best practices, including a failure to implement multi-factor authentication.

106. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

107. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

108. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and upon information and belief, Defendants failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

COMMON INJURIES & DAMAGES

109. As a result of Defendants' ineffective and inadequate data security practices, the

Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their Private Information; (e) invasion of privacy; and (f) the continued risk to their Private Information, which remains in the possession of Defendants, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

The Data Breach Increases Victims' Risk of Identity Theft

110. Plaintiff and Class Members are at a heightened risk of identity theft for years to come.

111. The unencrypted Private Information of Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted Private Information may fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the Private Information of Plaintiff and Class Members.

112. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

113. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity--or track the victim to attempt other crimes against the individual to obtain more data to perfect a crime.

114. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

115. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[36]

116. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with

[36] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/ (last visited on May 26, 2023).

an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals.

117. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

118. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the Data Breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiff and the other Class Members.

119. Thus, even if certain information (such as Social Security numbers) was not stolen in the Data Breach, criminals can still easily create a comprehensive "Fullz" package.

120. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Loss of Time to Mitigate Risk of Identity Theft and Fraud

121. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has

been lost.

122. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must monitor their financial accounts for many years to mitigate the risk of identity theft.

123. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as monitoring their accounts for fraudulent activity and checking their credit reports for unusual activity.

124. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") noting that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[37]

125. Plaintiff's mitigation efforts are also consistent with the steps FTC recommends data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[38]

126. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial

[37] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.
[38] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited July 7, 2022).

costs and time to repair the damage to their good name and credit record."[39]

Diminution Value of Private Information

127. PII and PHI are valuable property rights.[40] Their value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts including heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

128. An active and robust legitimate marketplace for Private Information exists. In 2019, the data brokering industry was worth roughly $200 billion.[41]

129. In fact, the data marketplace is so sophisticated that consumers can sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[42,43]

130. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[44]

131. Conversely sensitive PII can sell for as much as $363 per record on the dark web according to the Infosec Institute.[45]

---

[39] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Oct. 6, 2023) ("GAO Report").
[40] *See, e.g.,* Randall T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Private Information") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("Private Information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).
[41] https://www.latimes.com/business/story/2019-11-05/column-data-brokers
[42] https://datacoup.com/
[43] https://digi.me/what-is-digime/
[44] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html
[45] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/

132. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

133. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. Upon information and belief, the information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

134. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

135. The fraudulent activity resulting from the Data Breach may not come to light for years.

136. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendants' data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

137. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' network, amounting to over 1.16 million individuals'

(last visited Oct. 6, 2023).

detailed personal information, upon information and belief, and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

138. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

139. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes –*e.g.,* opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

140. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her personal information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

141. Consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

142. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendants' Data Breach.

Loss of the Benefit of the Bargain

143. Furthermore, Defendants' poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to entrust their valuable Private Information to Defendants and/or their agents for the provision of patient support services, Plaintiff and other reasonable consumers understood and expected that they were, in part, paying for the service and necessary data security to protect the Private Information, when in fact, Defendants did not provide the expected data security. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendants.

PLAINTIFF VANESSA HAY'S EXPERIENCE

144. Plaintiff Vanessa Hays is a current patient enrolled in Defendant Janssen's CarePath program.

145. To obtain patient support services from Defendant Janssen, she or her healthcare providers were required to provide her Private Information to Defendant Janssen.

146. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's Private Information in their systems.

147. Plaintiff is very careful about sharing her sensitive Private Information. Plaintiff stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff would not have entrusted her Private Information to Defendants had she known of Defendants' lax data security policies.

148. Upon information and belief, Plaintiff's PII and/or PHI was improperly accessed and obtained by unauthorized third parties in the Data Breach.

149. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including monitoring her accounts for fraudulent activity and checking her credit reports for unusual activity. Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

150. Despite these efforts, Plaintiff has noticed a marked uptick in spam messages since the Data Breach.

151. Plaintiff suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

152. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

153. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

154. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

155. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future data breaches.

CLASS ACTION ALLEGATIONS

156. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

157. Specifically, Plaintiff proposes the following class definitions, subject to amendment as appropriate:

> **Nationwide Class**
> All persons in the United States whose PII and/or PHI was compromised as a result of the Data Breach (the "Class").

158. Excluded from the Class are Defendants and their parents or subsidiaries, any entities in which they have a controlling interest, as well as their officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any judge to whom this case is assigned as well as their judicial staff and immediate family members.

159. Plaintiff reserves the right to modify or amend the definition of the proposed Class, as well as add subclasses, before the Court determines whether certification is appropriate.

160. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

161. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Although the precise number of such persons is currently unknown to Plaintiff and exclusively in the possession of Defendants, according to the Data Breach Today, at least 2.5

million persons were impacted in the Data Breach.[46] Thus, the Class is sufficiently numerous to warrant certification.

162. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendants engaged in the conduct alleged herein;

b. Whether Defendants' conduct violated the FTCA and/or HIPAA;

c. When Defendants learned of the Data Breach;

d. Whether Defendants' response to the Data Breach was adequate;

e. Whether Defendants unlawfully lost or disclosed Plaintiff's and Class Members' Private Information;

f. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

g. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

h. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

i. Whether Defendants owed a duty to Class Members to safeguard their Private Information;

[46] https://www.databreachtoday.com/group-claims-stole-25-million-patients-data-in-attack-a-23212 (last accessed Oct. 5, 2023).

j. Whether Defendants breached their duty to Class Members to safeguard their Private Information;

k. Whether hackers obtained Class Members' Private Information via the Data Breach;

l. Whether Defendants had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and the Class Members;

m. Whether Defendants breached their duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

n. Whether Defendants knew or should have known that its data security systems and monitoring processes were deficient;

o. What damages Plaintiff and Class Members suffered as a result of Defendants' misconduct;

p. Whether Defendants' conduct was negligent;

q. Whether Defendants were unjustly enriched;

r. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;

s. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

t. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

163. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the

Data Breach. Plaintiff's claims are typical of those of the other Class Members because, inter alia, all Class Members were injured through the common misconduct of Defendants. Plaintiff is advancing the same claims and legal theories on behalf of herself and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

164. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

165. Predominance. Defendants have engaged in a common course of conduct toward Plaintiff and Class Members in that all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

166. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, conducting this action as a class action presents far fewer management

difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

167. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Defendants have acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

168. Finally, all members of the proposed Class are readily ascertainable. Defendants have access to the names and addresses and/or email addresses of Class Members affected by the Data Breach.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

169. Plaintiff re-alleges and incorporates by reference paragraphs 1–168 as if set fully forth herein.

170. Defendant Janssen requires its patients, including Plaintiff and Class Members, to submit non-public Private Information in the ordinary course of providing its medical and patient support services.

171. Defendants gathered and stored Plaintiff's and Class Members' Private Information as part of their business of soliciting services to patients, which solicitations and services affect commerce.

172. Plaintiff and Class Members entrusted Defendant Janssen with their Private Information with the understanding that Defendant Janssen and its business associates, including Defendant IBM, would safeguard their information.

173. Defendants had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class Members could and would suffer if their Private Information

were wrongfully disclosed.

174. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendants had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendants' duty included a responsibility to implement processes by which they could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

175. Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair. .. practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

176. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

177. Defendants owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

178. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Defendant Janssen's patients. That special relationship arose because Plaintiff and the Class entrusted Defendant Janssen with their confidential Private Information, a necessary part of being part of the patient support program, run by Defendant Janssen.

179. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Private Information.

180. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiff or the Class.

181. Defendants also had a duty to exercise appropriate clearinghouse practices to remove former patients' Private Information if it was no longer required to retain pursuant to regulations.

182. Moreover, Defendants had a duty to promptly and adequately notify Plaintiff and the Class of the Data Breach.

183. Defendants had and continue to have a duty to adequately disclose that the Plaintiff's and Class Members' Private Information within Defendants' possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice is necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

184. Defendants breached their duties, pursuant to the FTC Act, HIPAA, and other applicable standards, and thus were negligent, by failing to use reasonable measures to protect

Class Members' Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failing to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

f. Failing to remove former patients' Private Information they were no longer required to retain pursuant to regulations;

g. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

h. Failing to secure their stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

185. Defendants violated Section 5 of the FTC Act and HPAA by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of Private Information obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

186. Plaintiff and the Class are within the class of persons that the FTC Act and HIPAA were intended to protect.

187. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act and HIPAA were intended to guard against.

188. Defendants' violation of Section 5 of the FTC Act and HIPAA constitutes negligence.

189. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

190. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

191. It was foreseeable that Defendants' failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

192. Defendants have full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and the Class could and would suffer if the Private Information were wrongfully disclosed.

193. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing Plaintiff's and Class Members' Private Information, the critical importance of providing adequate security of that Private Information, and the necessity

for encrypting Private Information stored on Defendants' systems.

194. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

195. Plaintiff and the Class had no ability to protect their Private Information that was in, and remains in, Defendants' possession.

196. Defendants were in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

197. Defendants' duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

198. Defendants have admitted that Plaintiff's and Class Members' Private Information was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

199. But for Defendants' wrongful and negligent breach of duties owed to Plaintiff and the Class, Plaintiff's and Class Members' Private Information would not have been compromised.

200. There is a close causal connection between Defendants' failure to implement security measures to protect Plaintiff's and Class Members' Private Information and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The Private Information of Plaintiff and the Class was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

201. As a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

202. As a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

203. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

204. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

205. Defendants' negligent conduct is ongoing, in that they still hold the Private Information of Plaintiff and Class Members in an unsafe and insecure manner.

206. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
Breach Of Implied Contract
(On Behalf of Plaintiff and the Class)

207. Plaintiff re-alleges and incorporates by reference paragraphs 1–168 as if set fully forth herein.

208. Plaintiff and Class Members were required to provide their Private Information to Defendants as a condition of receiving medical and patient support services from Defendant Janssen.

209. Plaintiff and the Class entrusted their Private Information to Defendants. In so doing, Plaintiff and the Class entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

210. Implicit in the agreement between Plaintiff and Class Members and the Defendants to provide Private Information, was the latter's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the Private

Information only under conditions that kept such information secure and confidential.

211. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and Defendants, on the other, are demonstrated by their conduct and course of dealing.

212. Defendant Janssen solicited, offered, and invited Plaintiff and Class Members to provide their Private Information as part of Defendant Janssen's regular business practices. Plaintiff and Class Members accepted Defendant Janssen's offers and provided their Private Information to Defendant Janssen, and entrusted that Defendant Janssen and its business associates, including Defendant IBM, would adequately and reasonably safeguard that Private Information.

213. In accepting the Private Information of Plaintiff and Class Members, Defendants understood and agreed that they were required to reasonably safeguard the Private Information from unauthorized access or disclosure.

214. On information and belief, at all relevant times Defendant Janssen promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiff and Class Members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.

215. On information and belief, Defendant Janssen further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' Private Information would remain protected.

216. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant Janssens's data security practices and the data security practices of its business associates, including Defendant IBM, complied with relevant laws and regulations and were consistent with industry standards.

217. Plaintiff and Class Members are third party beneficiaries of any contract between Defendant Janssen and Defendant IBM concerning the collection, management, maintenance, and storage of Plaintiff's and Class Members' Private Information.

218. Plaintiff and Class Members paid money to Defendant Janssen with the reasonable belief and expectation that Defendant Janssen and the business associates it paid, including Defendant IBM, would use part of their earnings to obtain adequate data security. Defendants failed to do so.

219. Plaintiff and Class Members would not have entrusted their Private Information to Defendants in the absence of the implied contract between them and Defendants to keep their information reasonably secure.

220. Plaintiff and Class Members would not have entrusted their Private Information to Defendants in the absence of their implied promise to monitor their computer systems and networks to ensure that they adopted reasonable data security measures.

221. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendants.

222. Defendants breached the implied contracts they made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

223. As a direct and proximate result of Defendants' breach of the implied contracts, Plaintiff and Class Members sustained damages, as alleged herein, including the loss of the benefit of the bargain.

224. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

225. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to, *e.g.*, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

226. Plaintiff re-alleges and incorporates by reference paragraphs 1–168 as if set fully forth herein.

227. This count is pleaded in the alternative to Plaintiff's breach of implied contract claim above (Count II).

228. Plaintiff and Class Members conferred a monetary benefit on Defendants. Specifically, they paid for services from Defendant Janssen and/or its agents and in so doing also provided Defendants with their Private Information. In exchange, Plaintiff and Class Members should have received from Defendants the services that were the subject of the transaction and should have had their Private Information protected with adequate data security.

229. Defendants knew that Plaintiff and Class Members conferred a benefit on them in the form their Private Information as well as payments made on their behalf as a necessary part of their receiving healthcare and patient support services from Defendant Janssen. Defendants appreciated and accepted that benefit. Defendants profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

230. Upon information and belief, Defendants fund their data security measures entirely from its general revenue, including payments on behalf of or for the benefit of Plaintiff and Class Members.

231. As such, a portion of the payments made for the benefit of or on behalf of Plaintiff and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendants.

232. Defendants, however, failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not provide adequate data security in return for the benefit Plaintiff and Class Members provided.

233. Defendants would not be able to carry out an essential function of their regular business without the Private Information of Plaintiff and Class Members and derived revenue by using it for business purposes. Plaintiff and Class Members expected that Defendants or anyone in Defendants' position would use a portion of that revenue to fund adequate data security practices.

234. Defendants acquired the Private Information through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

235. If Plaintiff and Class Members knew that Defendants had not reasonably secured their Private Information, they would not have allowed their Private Information to be provided to Defendants.

236. Defendants enriched themselves by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendants instead calculated to increase its own profit at the expense of

Plaintiff and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendants' decision to prioritize its own profits over the requisite security and the safety of their Private Information.

237. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money wrongfully obtained Plaintiff and Class Members, because Defendants failed to implement appropriate data management and security measures that are mandated by industry standards.

238. Plaintiff and Class Members have no adequate remedy at law.

239. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

240. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

241. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from

them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendants' services.

COUNT IV
Bailment
(*On Behalf of Plaintiff and the Class*)

242. Plaintiff re-alleges and incorporates by reference paragraphs 1–168 as if set fully forth herein.

243. Plaintiff and Class Members provided Private Information to Defendants—either directly or through healthcare providers and their business associates—which Defendants were under a duty to keep private and confidential.

244. Plaintiff's and Class Members' Private Information is personal property, and it was conveyed to Defendants for the certain purpose of keeping the information private and confidential.

245. Plaintiff's and Class Members' Private Information has value, and is highly prized by hackers and criminals. Defendants were aware of the risks it took when accepting the Private Information for safeguarding, and assumed the risk voluntarily.

246. Once Defendants accepted Plaintiff's and Class Members' Private Information, they were in the exclusive possession of that information, and neither Plaintiff nor Class Members could control that information once it was within the possession, custody, and control of Defendants.

247. Defendants did not safeguard Plaintiff's or Class Members' Private Information when they failed to adopt and enforce adequate security safeguards to prevent a known risk of a cyberattack.

248. Defendants' failure to safeguard Plaintiff's and Class Members' Private Information resulted in that information being accessed or obtained by third-party cybercriminals.

249. As a result of Defendants' failure to keep Plaintiff's and Class Members' Private Information secure, Plaintiff and Class Members suffered injury, for which compensation—including nominal damages and compensatory damages—is appropriate.

COUNT V
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

250. Plaintiff re-alleges and incorporates by reference paragraphs 1–168 as if set fully forth herein.

251. In light of the special relationship between Defendants and Plaintiff and Class Members, Defendants became a fiduciary by undertaking a guardianship of the Private Information to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendants do store.

252. Defendants had a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship with their patients, in particular, to keep secure their Private Information.

253. Defendants breached their fiduciary duty to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' Private Information.

254. Defendants breached their fiduciary duty to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

255. As a direct and proximate result of Defendants' breach of their fiduciary duty, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendants' services they received.

256. As a direct and proximate result of Defendants' breach of their fiduciary duty, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

C. For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to patient data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

D. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. Prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. Requiring Defendants to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. Requiring Defendants to delete, destroy, and purge the Private Information of Plaintiff and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. Requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class Members;

v. Prohibiting Defendants from maintaining the Private Information of Plaintiff and Class Members on a cloud-based database;

vi. Requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vii. Requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. Requiring Defendants to audit, test, and train its security personnel regarding any new or modified procedures;

ix. Requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

x. Requiring Defendants to conduct regular database scanning and securing checks;

xi. Requiring Defendants to establish an information security training program that includes at least annual information security training for all

patients, with additional training to be provided as appropriate based upon the patients' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. Requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. Requiring Defendants to implement a system of tests to assess its respective patients' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing patients' compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

xiv. Requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. Requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. Requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and

xvii. For a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Class, and to report any deficiencies with compliance of the Court's final judgment.

E. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

F. Ordering Defendants to pay for not less than ten years of credit monitoring services for Plaintiff and the Class;

G. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

H. For an award of punitive damages, as allowable by law;

I. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

J. Pre- and post-judgment interest on any amounts awarded; and

K. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: October 19, 2023

Respectfully Submitted,

/s/Steven M. Nathan
Steven M. Nathan
HAUSFELD LLP
33 Whitehall Street
Fourteenth Floor
New York, NY 10004
Tel. 646.357.1100
snathan@hausfeld.com

James J. Pizzirusso*
Amanda V. Boltax*
HAUSFELD LLP
888 16th Street N.W.
Suite 300
Washington, D.C. 20006
Tel. 202.540.7200
jpizzirusso@hausfeld.com
mboltax@hausfeld.com

Counsel for Plaintiff

** Pro Have Vice Forthcoming*

INTERNATIONAL BUSINESS MACHINES CORPORATION
Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

40068272000674297
000 0004419 00000000 0001 0002 02210 INS: 0 0

VANESSA HAYS
[redacted]

62
22210

September 15, 2023

Notice of Data Breach

Dear Vanessa Hays:

This notice concerns an incident involving unauthorized access to personal information contained within a database used on the Janssen CarePath platform, a patient support platform that offers savings options and other patient support resources.

International Business Machines Corporation ("IBM" or "we") is a service provider to Johnson & Johnson Health Care Systems, Inc. ("Janssen"). IBM manages the application and the third-party database that supports Janssen CarePath. We are writing to inform you of a recent incident that may have involved unauthorized access to your personal information stored in Janssen CarePath. While we have no reason to believe that your information has been misused, we want to let you know what happened and the steps we have taken in response. This letter explains what happened, our response, and steps you can take to protect your information.

What happened: Janssen recently became aware of a technical method by which unauthorized access to the database could be obtained. Janssen then immediately notified IBM, and, working with the third-party database provider, IBM promptly remediated the issue. IBM also undertook an investigation to assess whether there had been unauthorized access to the database. While IBM's investigation identified, on August 2, 2023, that there was unauthorized access to personal information in the database, the investigation was unable to determine the scope of that access. As a result, we are notifying you out of an abundance of caution.

What information was involved: The personal information involved in this incident may have included your name and one or more of the following: contact information, and information about medications and associated conditions that were provided to the Janssen CarePath application. Your Social Security number and financial account information were not contained in the database or affected.

What we are doing: After being informed of the issue by Janssen, IBM and the third-party database provider promptly identified and implemented steps that disabled the technical method at issue. IBM also worked with the third-party database provider to augment security controls to reduce the chance of a similar event occurring in the future.

What you can do: We encourage you to remain vigilant by regularly reviewing your account statements and explanations of benefits from your health insurer or care providers with respect to any unauthorized activity. If you identify services that you did not receive or other suspicious activity, promptly report that activity to the institution that provided the report. Additional information on steps that you can take to protect against potential misuse of personal information can be found in the enclosed "Additional Resources" document, which we encourage you to review.

AJ2151 v.08